JAVERBAUM WURGAFT HICKS KAHN WIKSTROM & SININS, P.C.
Stanley O. King
NJ Attorney ID: 034131996
1000 Haddonfield- Berlin Road, Suite 203
Voorhees, NJ 08043
Phone: (856) 596-4100

SPECTOR ROSEMAN & KODROFF, P.C.
William Caldes
Diana J. Zinser
Jeffrey L. Kodroff
Cary Zhang
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Telephone: (215) 496-0300

Counsel for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

JASON COLE, individually and on behalf of all others similarly situated, *Plaintiff*, v. GRAVY ANALYTICS, INC., VENNTEL, INC., and UNACAST INC., *Defendants*.	Civil Action No.: **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Jason Cole brings this class action on behalf of himself and all other similarly situated against Gravy Analytics, Inc., Venntel, Inc., and Unacast Inc. (together, "Defendants"). Plaintiff seeks monetary damages, restitution, and injunctive relief arising from a data breach that resulted in the theft of Plaintiff's highly sensitive personal data. Plaintiff makes the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation of their counsel, a review of public documents, including the Federal Trade Commission's ("FTC") complaint against Gravy Analytics and Venntel dated December 3, 2024, and other facts that are a matter of public record:

I. INTRODUCTION

1. In the modern age of technology, mobile phones are a pervasive part of the daily lives of Americans. Most American consumers always keep their phones near them, such that their phones go everywhere they go. Mobile phones are constantly tracking a user's location, generating records of a user's whereabouts at any given moment. This location data, and other personal information, is stored on the user's mobile phone.

2. The location signals captured identify consumers' precise geolocation by latitude and longitude coordinates and is extremely precise, identifying a consumer's location by within one meter of precision. This means the location signal is sufficiently precise to pinpoint not only what building a consumer is visiting, but even what room. Thus, it can reveal sensitive information such as medical conditions, sexual orientation, political activities and religious beliefs. When collected and analyzed across time, location data can indeed expose every aspect of a user's life.

3. Defendants are data brokers who amass and sell this raw location data to customers in both the private and public sectors, who are then privy to almost all facets of consumers' private

lives. In addition, Defendants use the data to identify consumers based on attributes and behaviors the data reveals, including sensitive attributes and behaviors, then discloses consumers' identities to third parties. Indeed, Defendants collect, process, and curate over 17 billion signals from approximately a billion mobile devices on a daily basis.

4. On January 4, 2025, a hacker revealed that it had hacked Defendants' systems and obtained millions of data points revealing locations of millions of individuals in the United States and Europe. The hacker posted screenshots as evidence and uploaded *17 terabytes* of data to a well-known online cybercrime forum, and threatened to post more if Defendants did not pay an undisclosed ransom.

5. This location data can be and is used to identify individuals and where they have been, including potentially sensitive locations such as places of worship, health care facilities, government buildings, and more.

6. According to independent cybersecurity experts who have reviewed the data, over 10,000 iOS and Android mobile applications were affected in the breach. These include some of the world's most popular apps such as Microsoft Outlook, Tinder, MyFitnessPal, and Candy Crush.

7. Plaintiff Jason Cole and millions of other consumers have been injured as a direct and proximate result of Defendants' failure to adequately secure consumers' sensitive location data. Plaintiff and the Class also face an imminent and substantial risk of further injuries. As a result, Plaintiff and the Class brings claims against Defendant for negligence, negligence *per se*, and statutory violations, seeking damages, declaratory relief, and injunctive relief.

II. PARTIES

A. Plaintiff

8. Plaintiff Jason Cole is a citizen of New Jersey and resides in Cherry Hill. Mr. Cole has a smartphone which he carries with him at all times and which he uses to access and use a number of mobile applications, including the Microsoft Outlook app.

9. Upon information and belief, Mr. Cole's location data has been collected by Defendants via his use of this and other apps.

10. Upon information and belief, Mr. Cole's location data collected by Defendants was affected by the data breach.

B. Defendants

11. Defendant Gravy Analytics, Inc. ("Gravy Analytics") is a Delaware corporation with its principal office or place of business located at 44679 Endicott Drive Suite 300, Ashburn, VA 20147.

12. Defendant Venntel, Inc. ("Venntel") is a Delaware corporation with its principal office or place of business located at 2201 Cooperative Way, Suite 600, Herndon, Virginia 20171. Venntel is a wholly-owned subsidiary of Gravy Analytics.

13. Defendant Unacast Inc. ("Unacast") is a Delaware corporation with its principal office or place of business located at 44679 Endicott Drive Suite 300, Ashburn, VA 20147. Gravy Analytics merged with Unacast in November 2023.

III. JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711 *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state

than the Defendants, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendant Gravy Analytics because Gravy Analytics has purposely availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

16. This Court has personal jurisdiction over Defendant Venntel because Venntel has purposely availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

17. This Court has personal jurisdiction over Defendant Unacast because Unacast has purposely availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District.

18. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District.

IV. STATEMENT OF FACTS

A. Background

19. Mobile phones are ubiquitous in the daily lives of Americans. Most consumers report keeping their phones near them at all times, meaning that their phones go everywhere that they go.

20. These devices are able to constantly track a user's location, generating records of a user's whereabouts throughout the day. Mobile phones are a source of personal information about their users, including personal information in the form of this location data.

21. Location data can expose sensitive information such as medical conditions, sexual orientation, political activities, and religious beliefs. When collected across time, this data can reveal every aspect of a consumer's life. Indeed, Defendants make this point in marketing material to potential customers, asserting that "Where we go is who we are."[1] This is more than just an advertising slogan for Defendants – it is the very point of their business.

22. Defendants amass and sell raw location data that tracks consumers' movements so that their customers can glean insights into consumers' private lives. In addition, Gravy Analytics also uses this data to identify consumers based on attributes and behaviors the data reveals, including sensitive and personal attributes and behaviors, and it then discloses this information to third parties.

23. Defendants obtain this location data not directly from consumers themselves, but rather from other data suppliers. These suppliers may themselves obtain the location data from other data suppliers, the mobile advertising marketplace, or mobile applications. Through these various suppliers, Defendants claim to "collect, process and curate" over *17 billion signals* from approximately a *billion mobile devices* on a daily basis.[2]

24. These location signals, gathered from consumers' mobile phones, identify consumers' precise geolocation by latitude and longitude coordinates at the time the signal was gathered.

---

[1] PRNewswire, "Gravy Analytics and AnalyticsIQ Empower Advertisers to Reach Affluent In-Market Consumers and Business Owners," *available at* https://www.prnewswire.com/news-releases/gravy-analytics-and-analyticsiq-empower-advertisers-to-reach-affluent-in-market-consumers-and-business-owners-300529352.html (last accessed Jan. 10, 2025).

[2] Complaint, *In the Matter of Gravy Analytics Inc. and Ventel Inc.*, Federal Trade Commission, No. 212-3035 (hereinafter "FTC Complaint") at 2, *available at* https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf.

25. Each location signal is also associated with a Mobile Advertising ID ("MAID") which is an alphanumeric identifier that iOS or Android platforms assign to each mobile device. This unique mobile device identifier is assigned to a consumer's mobile phone to assist marketers in advertising to consumers. These data signals are collected from a mobile device's GPS coordinates and may, at times, be augmented by other signals, such as WiFi.

26. The precision of the location signals gathered by Defendants is high. In its support documentation, Gravy Analytics states that location signals "should be at least 5 decimal places of precision."[3] The more decimal points in a location signal, the more precise the signal is. At 5 decimal points, the signal identifies a consumer's location to within approximately one meter of precision. This means the signal is sufficiently precise to identify not only what building a consumer is visiting, but even what room the consumer is in.

27. Defendants also tout the accuracy of their data. For example, Defendants assert that they have "implemented algorithms that process billions of data points daily [and] filter out unreliable signals," thus leaving Defendants with only data signals that they have been "verified as accurate."[4]

28. Defendants also explain that, when associating a data signal with a location, they use hand-drawn polygons (that is, using employees to draw the shape of the location being tracked) that "traces the walls of the venue," so that their data is "based on real people visiting real locations" without any "modeling."[5]

[3] *Id.*
[4] *Id.* at 2-3.
[5] *Id.*

B. Defendants Sell Consumers' Precise Location Data.

29. Defendants' business model is to compile massive amounts of mobile geolocation data collected from consumers and then disclose this information to third parties for a price. Gravy Analytics focuses on selling this information to commercial customers, while its subsidiary, Venntel, sells the information to public sector customers.

30. Defendants deliver data to their customers through file transfers at regular intervals, such as daily or weekly, or through providing access through an Application Programming Interface ("API"). In addition to continuously updating with new data, Defendants offer their customers the opportunity to search and receive at least three years of historical data.

31. Gravy Analytics sells multiple data products based on the consumer geolocation data it has compiled. For example, Gravy Analytics transfers raw precise mobile location data – that is timestamped latitude and longitude coordinates tied to, among other things, a MAID (or another persistent identifier) and IP address – to customers via batch deliveries through the cloud. Gravy Analytics offers data from as recent as the prior 48 hours to the previous year. Customers are able to schedule batch deliveries of location data based on requested criteria, such as geographic area or time.

32. Gravy Analytics also sells a tool that allows a marketer to "geo-fence" a location and obtain a list of MAIDs that were present at that location during a specific timeframe. For example, using this tool, a Gravy Analytics' customer could generate a list of MAIDs that attended a private event for a political cause. Gravy Analytics itself has used geo-fencing to create a list of MAIDs that visited specific churches and health-related events for customers.

33. Another tool tracks MAIDs that attend certain events, such as concerts or sporting events. Gravy Analytics asserts it "monitor[s] 1M+ local events."[6]

34. Gravy Analytics also transfers location data to its subsidiary, Venntel. Venntel sells the information to public sector customers, such as government contractors. Venntel sells location data associated with, among other things, a MAID or other persistent identifier, timestamp, IP address, and name of the app from which the location was collected.

35. Venntel also provides enhanced tools to its public sector customers to analyze and access consumers' location data. When a public sector customer accesses Venntel's data using one of these enhanced tools, Venntel typically associates the data with a unique persistent identifier that it refers to as a Venntel ID ("VID"). Venntel offers a tool that converts VIDs into MAIDs (and vice versa). Thus, the VID does not provide protections for consumers.

36. Venntel markets to its public sector customers that the location data and these enhanced tools can be used for government purposes.

37. The precise geolocation data, associated with MAIDs or other persistent identifiers, licensed, used, and sold by Defendants could be used to track consumers to sensitive locations, including places of religious worship, places that may be used to infer an LGBTQ+ identification, domestic abuse shelters, medical facilities, political activity, and welfare and homeless shelters. Indeed, Defendants themselves have tracked consumers to sensitive locations, including places of worship, political rallies, and locations associated with medical conditions or decisions.

[6] FTC Complaint at 3.

C. The Data Collected by Defendants Is Individually Identifiable and Sensitive.

38. The location data collected, used, and sold by Defendants is not anonymized and can easily be used to identify individuals. In fact, 95% of individuals can be positively identified with only four location data points.[7]

39. A persistent identifier, such as a MAID, is personally identifiable information. Defendants' geolocation data, combined with the mobile device's MAID or other persistent identifiers, identifies the mobile device's user or owner. Such identification occurs through several different methods.

40. First, the location data that Defendants collect, use, and sell typically includes multiple timestamped signals for each MAID or other persistent identifiers, which identifies many details about the mobile device owners.

41. For example, Venntel tells potential customers that "location data makes it possible to gain real-life insight into a device users' patterns-of-life (POL), locations visited and known associates."[8] Venntel further explains that, over a 90-day tracking of a "VIP Device," the company was able to identify the device user's "bed down location, work location, and visits to other USG [United States Government] buildings."[9] Additionally, in a "Quick Guide" document for one of its services, Venntel notes that where a device is located during the evening hours will show its customers when the consumer is at "home, gym, evening school, etc."[10]

---

[7] Rob Shavell, *The Skeleton Key to Our Lives: The Risks and Consequences of Consumer Location Data Tracking*, FORBES, Feb. 3, 2023, *available at* https://www.forbes.com/councils/forbestechcouncil/2023/02/03/the-skeleton-key-to-our-lives-the-risks-and-consequences-of-consumer-location-data-tracking/ (last accessed Jan. 14. 2025).
[8] *Id.* at 4.
[9] *Id.*
[10] *Id.*

42. Indeed, companies and other entities are using precise geolocation data to identify consumers and their activities. In one well-publicized example, a group used precise mobile geolocation data to identify by name a Catholic priest who visited LGBTQ+-associated locations, thereby exposing the priest's sexual orientation and forcing him to resign his position. As another example, journalists who purchased precise mobile geolocation from a data broker were able to track consumers over time and, as a result, identify several consumers, including 5 military officials, law enforcement officers, and others. One person the journalists were able to identify by name (and who confirmed her identity) was tracked attending a prayer service at a church.

43. Second, MAIDs and other persistent identifiers, by design, enable direct communication with individual consumers, are used to amass profiles of individuals over time and across different web and mobile services, and are the basis to make decisions and insights about individual consumers.

44. Finally, many businesses link consumers' MAIDs to other information about them, such as names, addresses, email addresses, and phone numbers. Indeed, at least one data broker that supplies geolocation data to Gravy Analytics specifically advertises a service that connects MAIDs to these other personally identifying points of information. Other data brokers advertise similar products.

D. Defendants' Collection, Use, and Sale of Consumers' Mobile Location Data Demonstrates the Value of Such Data.

45. The precise mobile location data collected, used, and sold by Defendants is sensitive and valuable information. Defendants use this data to target consumers based on the sensitive characteristics and behaviors that the location data reveals about consumers.

46. In addition to selling location data to customers for this use, Gravy Analytics itself also analyzes the data to create additional data products to sell to its customers. For example, Gravy

Analytics uses the data it collects to create "audience segments," or subsets of consumers who share interests or characteristics, including audience segments based on sensitive interests or characteristics. These groupings are formed based on the locations and events visited by mobile devices, combined with other information gathered about consumers, and allow Gravy Analytics' customers to identify and target consumers based on identified sensitive and personal interests or characteristics.

47. Gravy Analytics offers over 1100 audience segments with each segment made up of a list of MAIDs of consumers that meet the targeted interest or characteristic. These segments cover almost every aspect of a person's life, including eating and shopping habits, medical and health conditions, marital and family status, political leanings and activities, religious activities, and employment.

48. In addition, if a customer wishes to get specific information about individual consumers, Gravy Analytics also offers a "persona" data product in which it will provide a list of every audience segment connected to a specific MAID. For example, using the "persona" data product, a Gravy Analytics' customer could learn that a specific device MAID (e.g., 1234ABCD-1234- ABCD-1234-ABCD1234ABCD) is classified in the Gen X, Blue Collar Worker, ATM visitor, Parent of Teenagers, Golf Enthusiast, and Medicare Interest audience segments. Gravy Analytics claims to have associated over 250 million MAIDs of consumers with at least one audience segment.

49. The location data and the segments they are used to create are extremely valuable – an estimated *$12 billion* market.[11] Advertisers and other entities pay millions of dollars for

[11] Jon Keegan and Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, THE MARKUP, Sept. 30, 2021, *available at* https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data (last accessed Jan. 13, 2025).

location data and the insights that can be derived from them. For example, companies use location data to target ads to people who are physically near certain businesses.

50. Additionally, the federal government is a major purchaser of location data in the United States. The Department of Homeland Security ("DHS") and its subsidiaries, Immigrations and Customs Enforcement ("ICE") and Customs and Border Patrol ("CBP"), has paid Venntel at least $2 million to buy bulk location data. DHS, ICE, and CBP have used that data to track "suspicious" cellphone activity and to identify individuals for arrest and deportation.[12]

51. Location data is also valuable to criminals, who use it to launch location-based cyberattacks, commit fraud, identity theft, phishing, and other schemes. Cybercriminals may also use location data to stalk, intimidate, and organize attacks against victims, and to evade capture.[13]

E. FTC Complaint and Consent Order

52. On December 3, 2024, the FTC announced an enforcement action against Gravy Analytics and Venntel for their alleged misuse and unfair practices relating to their unlawful tracking of consumers' sensitive location data.[14]

53. In its complaint, the FTC accused Defendants of collecting, using, and selling consumers' location data without obtaining proper consent in violation of Section 5 of the FTC

[12] Bennett Cyphers, *How the Federal Government Buys or Cell Phone Location Data*, ELECTRONIC FRONTIER FOUNDATION, June 13, 2022, *available at* https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data (last accessed Jan. 13, 2025).

[13] IP Geolocation API, *How Cybercriminals Target You Based On Your Geolocation*, May 8, 2020, *available at* https://geo.ipify.org/blog/how-cybercriminals-target-you-based-on-your-geolocation (last accessed Jan. 14, 2025).

[14] *FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites*, FTC, Dec. 3, 2024, *available at* https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers (last accessed Jan. 14, 2025.)

Act. The FTC further alleged that Defendants continued to collect, use, and sell this data even after learning that they did not have consumers' informed consent.

54. The FTC recognized the location data at issue revealed sensitive information about consumers, including health and medical status, political activities, and religious affiliations. By collecting this information without consent, Defendants put consumers at risk of numerous harms, including physical violence, discrimination, and emotional distress.

55. Gravy Analytics and Venntel entered into a settlement with the FTC over the alleged privacy violations. Under the terms of the proposed settlement, Gravy Analytics and Venntell will be prohibited from selling, disclosing, or using sensitive location data.

F. Defendants' Privacy and Cybersecurity Policies

56. As companies that store and use sensitive consumer data including location data, Defendants are at high risk of cyberattacks. Defendants are well aware of this risk and expressly represent to customers that they will protect consumers' sensitive information.

57. Gravy Analytics' founder and CEO Jeff White has stated, "Consumer privacy has always been a cornerstone of our business," and "Consumer privacy is the responsibility of everyone in the location technology space, and we all need to do our part to ensure that the data we collect and use is privacy-friendly…[t]hat's why we're making the same, best-in-class, privacy-enhancing technology we use here at Gravy available to others that rely on location data."[15]

58. Defendants recognize the foreseeable risk of cyberattacks that they face. The risk that cybercriminals will breach Defendants' systems and gain unauthorized access to consumer location data and use that information for malicious purposes is not theoretical. As both Gravy

[15] PR Newswire, "Gravy Analytics Launches PrivacyCheck to Expand Its Industry-Leading Privacy Practices," Oct. 11, 2022, *available at* https://www.prnewswire.com/news-releases/gravy-analytics-launches-privacycheck-to-expand-its-industry-leading-privacy-practices-301645827.html (last accessed January 14, 2025).

Analytics' and Venntel's Privacy Polices state, "We have implemented appropriate administrative, technical, and physical safeguards to protect the information we collect from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. Please be aware that despite our best efforts, no data security measures can guarantee security."[16] [17]

59. Moreover, Defendants were on notice as to the potential weaknesses of its security practices as well as cybercriminals' desire to target their systems, as several large data breaches made international headlines in the past year, including the National Public Data breach by a cybercriminal group.[18]

60. Despite Defendants' duty to protect sensitive consumer location data, and the representations they made that they would do so, Defendants' data security practices fell short, leading to the Data Breach and compromise of consumer location data.

G. The Breach

61. At all relevant times, Defendants knew they were collecting and storing consumers' sensitive location data, and that, as a result, their systems would be attractive targets for cybercriminals. Indeed, cybercriminals did target and hack Defendants' systems, stealing massive amounts of data.

---

[16] *Privacy Policy*, VENNTEL, INC., effective Jan. 2023, *available at* https://web.archive.org/web/20241230151212/https://www.venntel.com/privacy-policy.
[17] *Privacy Policy*, GRAVY ANALYTICS, INC., effective Jan. 2023, *available at* https://web.archive.org/web/20230404145451/https://gravyanalytics.com/privacy-policy/.
[18] Pieter Arntz, *Massive Breach at Location Data Seller: "Millions" of Users Affected*, Jan. 9, 2025, *available at* https://www.malwarebytes.com/blog/news/2025/01/massive-breach-at-location-data-seller-millions-of-users-affected (last accessed Jan. 14, 2025); Pieter Arntz, *Stolen Data from Scraping Service National Public Data Leaked Online*, Aug. 8, 2024, *available at* https://www.malwarebytes.com/blog/news/2024/08/stolen-data-from-scraping-service-national-public-data-leaked-online (last accessed Jan. 14, 2025).

62. On January 7, 2025, tech website 404Media reported that hackers claimed to have stolen a "massive" amount of location data from Gravy Analytics and were threatening to publish it.[19]

63. The hack poses an enormous threat to individual consumers. As one cybersecurity expert stated:

> A location data broker like Gravy Analytics getting hacked is the nightmare scenario all privacy advocates have feared and warned about. The potential harms for individuals is haunting, and if all the bulk location data of Americans ends up being sold on underground markets, this will create countless deanonymization risk and tracking concerns for high risk individuals and organizations.[20]

64. On January 10, 2025, Norwegian state news NRK reported that Gravy Analytics had submitted a deviation report to the Norwegian Data Protection Authority on January 4, 2025.[21]

65. In the report, Gravy Analytics stated that it had discovered that "an unauthorized person appears to have gained unauthorized access to the Gravy Analytics [Amazon Web Services] environment through a misappropriated access key."[22]

66. Gravy Analytics confirmed that the unauthorized person "obtained some files" but stated that "the contents of those files and whether they contain personal data remains under investigation."[23]

---

[19] Joseph Cox, *Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data*, Jan. 7, 2025, *available at* https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/ (last accessed Jan. 13, 2025).
[20] *Id.*
[21] NRK, "Data breach detected when hacker contacted," *available at* https://www.nrk.no/norge/oppdaget-datainnbrudd-da-hackeren-tok-kontakt-1.17201694 (last accessed Jan. 13, 2025).
[22] "Confidential Notification of a Personal Data Breach to the Norwegian Data Protection Authority," *available at* https://fido.nrk.no/8a09133d2b14a7e72c31006ef2611b22fd78d7c6bfd7cc62f7d35f13b3c2d338/Datatilsynet_Unacast_Security%20Incident%20Notification_Redacted.pdf (last accessed Jan. 13, 2025).
[23] *Id.*

67. While Gravy Analytics would not elaborate on the "contents" of the files, the hacker did, bragging about the exploits on a notorious Russian cybercrime forum called XSS:

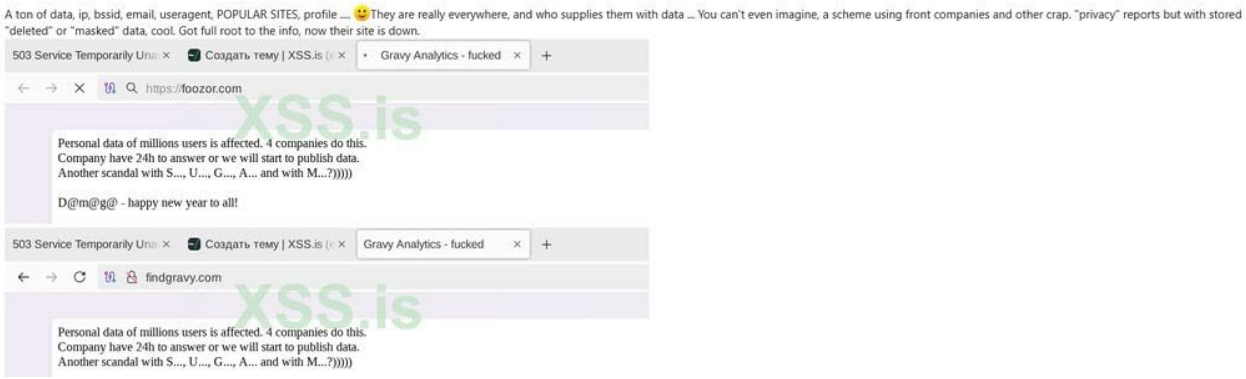

Figure 1: Screenshot from XSS[24]

68. Posting on Gravy Analytics websites, the hacker stated that "Personal data of millions users is affected" and that Gravy Analytics "have 24h to answer or we will start to publish data."[25]

69. As of the filing of this complaint, Defendants have not officially reported the breach to authorities in the United States.

V. THE DATA BREACH IS LIKELY TO CAUSE SUBSTANTIAL INJURY TO CONSUMERS

70. The instant Plaintiff's and Class Members' location data was accessed and obtained by a third party without their consent or authorization, Plaintiff and Class Members suffered injury from a loss of privacy.

71. As a result of the Data Breach, Plaintiff and Class Members have been further injured by the damages to and loss in value of their location data—a form of intangible property

[24] Cox, *supra* n. 19.
[25] *Id.*

with inherent value that Plaintiff and Class Members were deprived of when it was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

72. Given the nature of the location data involved and the malicious and intentional means through which the information was stolen, the Data Breach has also caused Plaintiff and Class Members to suffer imminent harm arising from a substantially increased risk of fraud, financial crimes, and crimes of intimidation which may arise from their locations being in the hands of criminals, as a direct and proximate result of Defendants' misconduct.

73. Identification of private and sensitive characteristics of consumers from the location data Defendants failed to protect from malicious actors is also likely to injure consumers through exposure to blackmail, stigma, discrimination, physical violence, and other harms.

74. The substantial risk of imminent harm and loss of privacy have also caused Plaintiff and Class Members to suffer stress, fear, emotional distress, and anxiety.

75. The substantial risk of imminent harm, loss of privacy, stress, fear, emotional distress, and anxiety is starkly real. As described above, the location data involved in the Gravy Analytics breach may be used to identify individual consumers and their visits to sensitive locationg. The fact that malicious actors have obtained this data poses an unwarranted intrusion into the most private areas of consumers lives and has caused or is likely to cause substantial injury to consumers.

76. For example, one of the apps affected by this breach is Momly, a pregnancy tracking app. Location data obtained from a phone with this app could be used to identify individuals who have visited an abortion clinic and who have had or may have contemplated having an abortion. As described above, it is possible to identify a mobile device that visited an abortion clinic and trace that mobile device to a residence.

77. Another example of an app affected by the breach is Sobriety Counter, an app used by individuals battling addiction. Location data obtained from a phone with this app could be used to identify individuals who have visited addiction recovery centers or meetings.

78. Outlogic (formerly known as X-Mode), a company that collects location data through apps, collected data from Muslim prayer apps and sold it to military contractors.[26]

79. Additionally, the location data exposed by the Data Breach is extremely valuable. In fact, the location data market was valued at $21.21 billion in 2024, with the value only expected to increase.[27] Outlogic's license for a location dataset costs $240,000 per year.[28]

VI. CLASS ACTION ALLEGATIONS

80. Plaintiff brings this action individually and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "the Class" or "Class Members."

81. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiff proposes the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

> **Nationwide Class**: All natural persons residing in the United States whose location data was compromised as a result of the Data Breach.
>
> **New Jersey Subclass**: All natural persons residing in New Jersey whose location data was compromised as a result of the Data Breach.

---

[26] Jon Keegan and Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, THE MARKUP, Sept. 30, 2021, *available at* https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data (last accessed Jan. 13, 2025).

[27] Grand View Research, "Location Intelligence Market Size & Trends," *available at* https://www.grandviewresearch.com/industry-analysis/location-intelligence-market (last accessed Jan. 14, 2025).

[28] Jon Keegan and Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, THE MARKUP, Sept. 30, 2021, *available at* https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data (last accessed Jan. 13, 2025).

82. Excluded from the Class are: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

83. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

84. **Numerosity**. The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Class likely consists of thousands if not millions of individuals who can be identified through Defendants' records.

85. **Typicality**. Plaintiff's claims are typical of the claims of other members of the Class because they arise from the same conduct by Defendants, are based on the same legal theories, and Plaintiff's location data, like that of every class member, was compromised in the Data Breach.

86. **Adequacy**. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel competent and experienced in complex litigation and class actions. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of members of the Class and have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Class.

87. **Commonality**. The Class's claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not limited to:

a. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the location data compromised in the Data Breach;

b. Whether Defendants data security protocols prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendants' data security protocols prior to and during the Data Breach were consistent with industry standards;

d. Whether Defendants each owed a duty to Class Members to safeguard their location data;

e. Whether Defendants breached their duties to Class Members to safeguard their location data;

f. Whether cyberhackers obtained, sold, copied, stored or released Class Members' location data;

g. Whether Defendants knew or should have known that their data security programs and monitoring processes were deficient;

h. Whether and when Defendants actually learned of the Data Breach;

i. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their location data was compromised;

j. Whether Defendants violated the law by failing to adequately, promptly, and accurately inform Plaintiff and Class Members that their location data was compromised;

k. Whether the Class Members suffered legally cognizable damages as a result of Defendants' misconduct; and

l. Whether Plaintiff and Class Members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

88. **Predominance**. Defendants have each engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and the Class Members' data at issue here was stored by Defendants and was accessed during the Data Breach. The common issues

arising from Defendants' conduct affecting Class Members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

89. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

VII. CAUSES OF ACTION

COUNT 1: NEGLIGENCE

(On behalf of Plaintiff and the Nationwide Class)

90. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

91. Defendants owed a duty under common law to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the location data in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

92. More specifically, this duty included:

a. Designing, maintaining, and testing Defendants' security systems to ensure that Plaintiff's and Class members' location data in their possession was adequately protected;

b. Implementing processes that would detect a breach of their security systems in a timely manner;

c. Timely acting upon warning and alerts, including those generated by their own security systems, regarding intrusions upon their networks and systems;

d. Maintaining security measures consistent with industry standards;

e. Exercising appropriate discretion in selecting third-party vendors to whom they make Plaintiff's and Class members' location data available; and

f. Timely rectifying known vulnerabilities in its networks or systems.

93. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

94. Defendants have a common law duty to prevent foreseeable harm to others. This duty exists because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendants. By obtaining, maintaining, and handling valuable sensitive information that is routinely targeted by criminals for unauthorized access and use for nefarious purposes, including sensitive location data, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

95. Defendants also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendants' conduct included their actions to intentionally obtain sensitive location data, and their failure to adequately restrict access to the networks and systems that held Plaintiff's and Class members' location data, as Defendants knew it was more likely than not that Plaintiff and Class members would be harmed if Defendants allowed a breach of their computer networks and systems.

96. Defendants have admitted that they have a responsibility to protect consumer data they are entrusted with.

97. Further, Defendants' duty arose from various statutes requiring them to implement reasonable data security measures, including but not limited to Section 5 of the FTC Act. Section 5 requires Defendants to take reasonable measures to protect Plaintiff's and Class members' sensitive data. Section 5 prohibits unfair practices in or affecting commerce, including, as interpreted and enforced by the FTC, the unfair act or practice of businesses like Defendants failing to use reasonable measures to protect highly sensitive data. Therefore, Defendants were required and obligated to take reasonable measures to protect data they possessed, held, or otherwise used.

98. Defendants' independent duty is untethered to any contractual relationship between Defendants and Plaintiff or Defendants and Class members and does not require a contractual relationship.

99. Defendants breached the duties owed to Plaintiff and Class members and were thus negligent. Although the exact methodologies employed by the unauthorized third parties are unknown to Plaintiff at this time, on information and belief, Defendants breached their duties through some combination of the following errors and omissions that allowed the data compromise to occur: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information that resulted in the unauthorized access and compromise of location data; (b) mishandling their data security by failing to assess the sufficiency of their safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security program in light of the circumstances alleged

herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow their own privacy policies and practices; (h) failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive location information; and (i) failing to timely patch known vulnerabilities in their computer systems and networks.

100. But for Defendants' wrongful and negligent breach of the duties owed to Plaintiff and the Class, their location data would not have been compromised.

101. Failure to implement adequate security measures to protect the sensitive location data of Plaintiff and Class members created conditions conductive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class members' location data.

102. Plaintiff and Class members were the foreseeable victims of Defendants' inadequate data security measures, and it was also foreseeable that Defendants' failure to protect Plaintiff's and Class members' location data would result in injury to Plaintiff and Class members.

103. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members have suffered injuries, including theft of their location data and diminution of the value of same, violation of their privacy, and substantial risk of experiencing physical violence, discrimination, and emotional distress related to the exposure of sensitive personal characteristics related to their location data.

104. As a direct and proximate result of Defendants' negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages in an amount to be proven at trial.

COUNT 2: NEGLIGENCE PER SE

(On behalf of Plaintiff and the Nationwide Class)

105. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

106. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendants for failing to use reasonable measures to protect consumer location data. Various FTC publications and orders also form the basis of Defendants' duty.

107. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect location data and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of location data it obtained and stored and the foreseeable consequences of a data breach involving companies as large as Defendants, including the damages that would result to Plaintiff and Class Members.

108. Defendants' violations of Section 5 of the FTC Act constitutes negligence *per se*.

109. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

110. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against.

111. Defendants breached their duties to Plaintiff and Class Members under Section 5 of the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' location data. Plaintiff and Class Members were foreseeable victims of Defendants' violations of Section 5 of the FTC Act. Defendants also knew or should have known that its failure to implement reasonable data security

measures to protect and secure Plaintiff's and Class Members' location data would cause damage to Plaintiff and Class Members.

112. But for Defendants' violation of the applicable laws and regulations, Plaintiff's and Class Members' location data would not have been compromised by unauthorized third parties.

113. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and Class Members have been injured as described herein and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 3: DECLARATORY JUDGMENT

(On behalf of Plaintiff and the Nationwide Class)

114. Plaintiff restates and realleges all foregoing factual allegations as if fully set forth herein.

115. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

116. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' location data and whether Gravy Analytics and Venntel are each currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their location data Plaintiff allege that Gravy Analytics' and Venntel's respective data security measures remain inadequate. Furthermore, Plaintiff and Class Members continue to suffer injury as a result of the compromise of their location data and remain at imminent risk that further compromises of their location data will occur for as long as Gravy Analytics and Venntel each maintain inadequate data security measures.

117. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Gravy Analytics owes a legal duty to secure consumers' location data under the common law, Section 5 of the FTC Act;

b. Venntel owes a legal duty to secure consumers' location data under the common law and Section 5 of the FTC Act;

c. Gravy Analytics continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' location data; and

d. Venntel continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class Members' location data.

118. This Court also should issue corresponding prospective injunctive relief requiring Gravy Analytics and Venntel to each employ adequate security protocols consistent with law and industry standards to protect consumers' location data.

119. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Gravy Analytics or Venntel, or a similar entity. The risk of another such breach is real, immediate, and substantial. If another breach at Gravy Analytics, Venntel, or a similar entity occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

120. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Gravy Analytics or Venntel if an injunction is issued. Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Gravy Analytics and Venntel of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Gravy Analytics and Venntel each have a pre-existing legal obligation to employ such measures.

121. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by preventing another data breach at Gravy Analytics, Venntel, or a similar entity, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

COUNT 4: NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT N.J. Stat. Ann. §§ 56:8-163, *et seq*.

(On behalf of Plaintiff and the New Jersey Subclass)

122. Plaintiff, individually and on behalf of the New Jersey Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein

123. Gravy Analytics and Venntel are each businesses that compile or maintain computerized records that include "personal information" on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

124. Plaintiff's and New Jersey Sub Class Members' location data includes "personal information" covered under N.J. Stat. Ann. §§ 56:8-163, et seq.

125. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person."

126. Because Defendants discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the location was not secured, Defendants had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, et seq.

127. By failing to disclose the Data Breach in a timely and accurate manner, Defendants violated N.J. Stat. Ann. § 56:8-163(b).

128. As a direct and proximate result Defendants' violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass Members suffered the damages described above.

129. Plaintiff and New Jersey Subclass Members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT 5: NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. §§ 56:8-1 *et seq.*

(On behalf of Plaintiff and the New Jersey Subclass)

130. Plaintiff, individually and on behalf of the New Jersey Subclass, restate and reallege all foregoing factual allegations as if fully set forth herein

131. Gravy Analytics is "person" as defined by N.J. Stat. Ann. § 56:8-1(d).

132. Venntel is a "person" as defined by N.J. Stat. Ann. § 56:8-1(d).

133. Gravy Analytics and Venntel sell "merchandise" as defined by N.J. Stat. Ann. § 56.8-1(c) and (e).

134. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1 et seq. prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

135. Defendants' unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and New Jersey Subclass members' location data, which was a direct and proximate cause of the data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass members' location data, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of consumers' location data, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of consumers' location data, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify the Plaintiff and New Jersey Subclass members of the data breach

g. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and New Jersey Subclass members' location data; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass members' location data, including duties imposed by the FTC Act, 15 U.S.C.

136. Defendants' misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and their ability to protect the confidentiality of consumers' location data.

137. Defendants intended to mislead Plaintiff and New Jersey Subclss members and induce them to rely on their misrepresentations and omissions.

138. Defendants acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff's and New Jersey Subclass members' rights.

139. As a direct and proximate result of Defendants' unconscionable and deceptive practices, Plaintiff and New Jersey Subclass members have suffered and will continue to suffer injury, loss of money or property, and monetary and non-monetary damages

VIII. REQUEST FOR RELIEF

Plaintiff, individually and on behalf of members of the Class and Subclass, as applicable, respectfully requests that the Court enter judgment in their favor and against Defendants as follows:

A. That this Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff are proper class representatives; and appoint Plaintiff's Co-Lead Interim Class Counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendants from continuing to engage in the unlawful acts, omissions, and practices described herein, including:

   i. Prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

   ii. Requiring Defendants to protect all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   iii. Requiring Defendants to delete, destroy and purge the location data of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendants to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of Plaintiff' and Class Members' location data;

v. Requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to each promptly correct any problems or issues detected by such third-party security auditors;

vi. Requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. Requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

viii. Requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants network is compromised, hackers cannot gain access to other portions of Defendants' systems;

ix. Requiring Defendants to conduct regular database scanning and security checks;

x. Requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon employees' respective responsibilities with handling

location data, as well as protecting the location data of Plaintiff and Class Members;

xi. Requiring Defendants to routinely and continually conduct internal training and education, at least annually, to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. Requiring Defendants to implement a system of testing to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs and systems for protecting location data;

xiii. Requiring Defendants to implement, maintain, regularly review and revise as necessary, a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xiv. Requiring Defendants to meaningfully educate all Class Members about the threats they face as a result of the loss of their location data to third parties, as well as the steps affected individuals must take to protect themselves;

xv. Requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xvi. Appointing a qualified and independent third-party assessor to conduct for a period of 10 years a SOC 2 Type 2 attestation to evaluate on an annual basis Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies in compliance with the Court's final judgment.

C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

D. For an award of actual damages, compensatory damages, statutory damages, nominal damages, and statutory penalties, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including reasonable expert witness fees;

G. For an award of pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

IX. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated: January 14, 2025

Respectfully submitted,

/s/ Stanley O. King

JAVERBAUM WURGAFT HICKS KAHN WIKSTROM & SININS, P.C.
Stanley O. King
NJ Attorney ID: 034131996
1000 Haddonfield- Berlin Road, Suite 203
Voorhees, NJ 08043
Phone: (856) 596-4100
sking@lawjw.com

SPECTOR ROSEMAN & KODROFF, P.C.
William Caldes
Diana J. Zinser
Jeffrey L. Kodroff
Cary Zhang
2001 Market Street, Suite 3420
Philadelphia, PA 19103
Phone: (215) 496-0300
bcaldes@srkattorneys.com
dzinser@srkattorneys.com
jkodroff@srkattorneys.com
czhang@srkattorneys.com

Attorneys for Plaintiff and the Proposed Class